MICHAEL F. RAM
CALIFORNIA BAR NO: 104805
MRAM@FORTHEPEOPLE.COM
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 VAN NESS AVE, STE 500,
SAN FRANCISCO, CA, 94102-3275
T: (415) 846-3862

John A. Yanchunis*
JYanchunis@forthepeople.com
(*Pro Hac Vice forthcoming)*
Ronald Podolny*
ronald.podolny@forthepeople.com
(*Pro Hac Vice forthcoming)*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SHANNON LECHELE HARKER, individually and on behalf of all others similarly situated, Plaintiff, v. **PROGRESS SOFTWARE CORPORATION AND DELTA DENTAL OF CALIFORNIA,** Defendants.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Shannon Lechele Harker ("Harker"), individually and on behalf of all others similarly situated, brings this action against Progress Software Corporation ("PSC") and Delta Dental of California ("Delta Dental"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold the Defendants responsible for the injuries the Defendants inflicted on Plaintiff and millions of similarly situated persons ("Class Members") due to the Defendants' impermissibly inadequate data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized access by cybercriminals (the "Data Breach" or "Breach") on or about June 1, 2023. Upon information and belief, the cybercriminals who perpetrated the Breach are part of the Clop crime group,[1] which was notorious in cyber security circles prior to the Data Breach.[2]

2. Defendant Delta Dental of California ("Delta Dental") is a leading dental insurance provider. Together with its affiliates, it provides dental benefits to more than 45 million people across 15 states. Delta Dental is headquartered in San Francisco, CA.[3]

---

[1] Mathew J. Schwartz, "Latest MOVEit Data Breach Victim Tally: 455 Organizations", https://www.bankinfosecurity.com/latest-MOVEit-data-breach-victim-tally-455-organizations-a-22650 (last accessed on March 18, 2024).

[2] "Ransomware spotlight: Clop" (February 22, 2022), https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop (last accessed on March 18, 2024).

[3] Dun & Bradstreet, https://www.dnb.com/business-directory/company-profiles.delta_dental_of_california.cdec6545240f5a381612d477d055bf6e.html (last visited on March 18, 2024).

Defendant Delta Dental is a member organization of Delta Dental Plans Association, a not-for-profit organization which operates America's largest network of dental insurance companies.[4]

3. Defendant PSC is a Massachusetts-based software company that offers, among others, the "MOVEit" cloud hosting and file transfer service, which was the subject of the Data Breach.

4. Delta Dental utilized PSC's MOVEit service to transfer or store its clients' sensitive information, which was stolen by cybercriminals.

5. The data which the Defendants collected from the Plaintiff and Class Members, and which was exfiltrated by cybercriminals from the Defendants, were highly sensitive. Upon information and belief, the exfiltrated data included personal identifying information ("PII") like individuals' names, health insurance and treatment information.

6. Upon information and belief, prior to and through the date of the Data Breach, the Defendants obtained Plaintiff's and Class Members' PII and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, PSC inadequately maintained its network, platform, software, and technology partners—rendering these easy prey for cybercriminals. As evidenced by the Data Breach, Delta Dental performed inadequate, if any, due diligence before selecting PSC's unsecure product for the storage of its clients' PII and other sensitive information.

[4] Delta Dental, "About Us", https://www.deltadental.com/us/en/about-us.html#:~:text=Delta%20Dental%20serves%20more%20than,quick%20answers%20and%20personalized%20service (last accessed March 18, 2024).

7. Upon information and belief, the risk of the Data Breach was known to the Defendants. Thus, the Defendants were on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

8. Then, after the Data Breach, the Defendants failed to provide timely notice to the affected Plaintiff and Class Members—thereby exacerbating their injuries. Ultimately, the Defendants deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, the Defendants impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

9. Even when the Defendants finally notified Plaintiff and Class Members of their PII's exfiltration, the Defendants failed to adequately describe the Data Breach and its effects.

10. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of the Defendants' negligence. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial accounts.

11. Armed with the PII stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

12. Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

14. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose PII were exfiltrated and compromised in the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

16. Plaintiff Shanon Lechele Harker is a natural person and resident and citizen of Texas.

17. Defendant PSC is a Massachusetts corporation with its headquarters and principal place of business located in Burlington, Massachusetts.

18. Defendant Delta Dental is a leading insurance provider serving more than 45 million members.[5] Delta Dental network includes affiliates Delta Dental Insurance Company, Delta Dental of Pennsylvania and Delta Dental of New York, Inc., and provides dental benefits to more than 45 million people across 15 states, the District of Columbia, Puerto Rico, and the Virgin Islands. Delta Dental is headquartered in San Francisco, CA.[6] Delta Dental is a member of "Delta Dental Plans Association," a national association of dental insurers.[7]

JURISDICTION AND VENUE

19. This Court has original subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiff (and many members of the class) are citizens of states different than that of PSC and Delta Dental.

20. This Court has personal jurisdiction over PSC because PSC regularly conducts substantial business in this District.

---

[5] "Forbes names Delta Dental of California one of America's best employers for 2024", https://www1.deltadentalins.com/newsroom/releases/2024/03/forbes-names-delta-dental-of-ca-one-of-americas-best-employers-for-2024.html (May 1, 2024) (last accessed on March 18, 2024).

[6] Dun & Bradstreet, Delta Dental of California, https://www.dnb.com/business-directory/company-profiles.delta_dental_of_california.cdec6545240f5a381612d477d055bf6e.html (last visited on March 18, 2024).

[7] Delta Dental, "About Us", https://www.deltadental.com/us/en/about-us.html#:~:text=As%20the%20nation's%20leading%20provider,not%2Dfor%2Dprofit%20organization. (Last accessed March 18, 2024).

21. This Court has personal jurisdiction over Delta Dental because Delta Dental maintains its principal place of business in this district.

22. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, Defendant Delta Dental maintains its principal place of business in the jurisdiction, and Defendant PSC conducts substantial business in this District.

FACTUAL ALLEGATIONS

Defendants Collected and Stored the PII of Plaintiff and Class Members

23. PSC is a software company that offers a wide range of software products and services to corporate and governmental entities throughout the United States and the world, including cloud hosting and allegedly secure file transfer services such as MOVEit.

24. Upon information and belief, numerous consumer-facing entities used PSC for information technology management and software services, including PSC's file transfer software, MOVEit. One of these entities was Delta Dental. Within this relationship, Delta Dental transferred and entrusted data, including Plaintiff's and Class Members PII, to PSC.

25. Upon information and belief, PSC received and maintained the PII of its customers' customers, such as individuals' names, addresses, dates of birth, and Social Security numbers. These records are stored on PSC's and its partners' computer systems.

26. Upon information and belief, PSC's file transfer software, MOVEit, was hacked by the Clop crime group, which was notorious prior to the Data Breach,[8] resulting in the Breach and the exfiltration of customer PII, including Plaintiff's and Class Members PII.

27. Because of the highly sensitive and personal nature of the information Defendants acquire and store, Defendants knew or reasonably should have known that they stored protected PII and must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' PII and provide adequate notice to customers if their PII is disclosed without proper authorization.

28. When Defendants collect this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

29. Defendants acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' PII.

30. Upon information and belief, Delta Dental made no, or insufficient, efforts to ensure that PSC complied with the requisite data security standards, and all federal and state laws regarding PII protection, before selecting PSC to store its clients' data.

31. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew, or should have known, that they were thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

---

[8] "Ransomware spotlight: Clop" (February 22, 2022), https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop (last accessed on March 18, 2024).

32. On PSC's website, PSC represents that,

a. "Progress Software Corporation, together with all of its subsidiaries and affiliates, ('Progress Software', 'we', 'us', 'our' or the 'Company') is committed to protecting the privacy of individuals who visit the Company's web sites, individuals who register to use our services, and individuals who register to attend the Company's corporate events."

b. "Progress implemented technical and organizational measures to ensure HIPAA compliance and operates in secure computing environments in its corporate offices, development environments, and production cloud products. Progress audits its security solutions and processes annually to maintain SOC2 and HIPAA validation."[9]

33. Upon information and belief, PSC represented to its customers orally and in written contracts, marketing materials, and otherwise that it would properly protect all PII it obtained. Upon information and belief, PSC knew or reasonably should have known that these representation regarding protecting PII and PHI would be passed on to its customers' customers, such as Delta Dental's insureds.

34. Delta Dental, similarly, represented to its customers: "security is important to both Delta Dental and you, we employ reasonable safeguards designed to promote the security of our systems and protect your personal information from unauthorized destruction, use, modification, or disclosure. Personal information is protected using

[9] "Privacy at Progress", https://www.progress.com/legal/privacy-center (last accessed on March 18, 2024); "Privacy Policy. Last update: Effective October 25, 2023", https://www.progress.com/legal/privacy-policy (last accessed on March 18, 2024).

various physical, administrative and/or technical safeguards in transit and at rest." Specifically in respect of PII, Delta Dental represented as follows: "Where your dental coverage benefits are underwritten or administered by a Delta Dental Company, Delta Dental collects, uses, and discloses your individually identifiable health information consistent with the HIPAA Notice of Privacy Practices pertaining to your dental plan."[10] Upon information and belief, the "Notice of Privacy Practices" was not accessible at the material time, and an error message was displayed instead.[11]

35. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

36. Upon information and belief, Plaintiff and Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

37. PSC could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners. Delta Dental could have prevented or mitigated the

[10] Delta Dental, "Privacy Statement for the Delta Dental Plans Association Website and Mobile App – Consumers", https://www.deltadental.com/us/en/about-us/privacy-policy.html (Last accessed March 13, 2024).
[11] Delta Dental, "Page Not Found", https://www.deltadentalins.com/HIPAA/HIPAAprivacy.html (Last accessed March 13, 2024).

effects of the Data Breach by selecting a services provider that employs reasonable security measure to protect its customers' information.

38. Defendants' negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

39. Despite the prevalence of public announcements of data breaches and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

40. Delta Dental failed to conduct the necessary inquiries into PSC's data security practices, and selected PSC, which had inadequate information security practices, as its data storage services provider.

41. PSC failed to properly select its information security partners.

42. PSC failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

43. PSC failed to ensure the proper monitoring and logging of file access and modifications.

44. PSC failed to ensure the proper training its and its technology partners' employees as to cybersecurity best practices.

45. PSC failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

46. Delta Dental and PSC failed to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

47. PSC knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII.

48. Defendants failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and potentially disclose it to others without consent.

49. Upon information and belief, PSC failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions. Upon information and belief, Delta Dental failed to ensure that PSC had implemented such processes before selecting PSC as its services provider.

50. Upon information and belief, PSC failed to ensure the proper encryption of Plaintiff's and Class Members' PII and monitor user behavior and activity to identify possible threats. Upon information and belief, Delta Dental failed to ensure that PSC employed encryption in a reasonable manner, or at all, before selecting PSC as its services provider.

The Data Breach

51. On or about May 31, 2023, PSC posted a notice on its website stating that it had found a vulnerability in its MOVEit Transfer and MOVEit Cloud applications that allowed an unauthorized third party to access Plaintiff's and Class Member's PII. In an associated notice on the National Vulnerability Database, PSC provided further detail:[12]

[12] "MOVEit Transfer and MOVEit Cloud Vulnerability", https://www.progress.com/security/MOVEit-transfer-and-MOVEit-cloud-vulnerability (last visited on March 18, 2024). See also: National Vulnerability Database, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34362 (last visited on March 18, 2024).

> In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that **could allow an unauthenticated attacker to gain access to MOVEit Transfer's database**. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), **an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements**. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. **All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected**, including older unsupported versions. (Emphasis added)

52. Although PSC claims to have notified its customers immediately upon learning of the vulnerability, Delta Dental did not notify its own customers of the Data Breach until January 12, 2024. On or about that date, Harker received a letter entitled "Notice of Data Security Incident", stating that Delta Dental's customers' data had been compromised in a Data Breach suffered by PSC, and informed them of the following:

> Delta Dental of California and affiliates ("Company") experienced a data security incident involving the MOVEit Transfer ("MOVEit") software, an application used by our company and many organizations worldwide. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter provides information about what happened, how to help protect your information and resources offered to assist you.
>
> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more.
>
> On June 1, 2023, the Company learned that unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. WE stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. WE also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity and

ransomware activity.

> On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third party experts in computer forensics, analytics and data mining to determine what information was impacted and with whom it is associated.
>
> This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement o the incident and have been cooperating with them since.

53. The Notice of Data Breach enumerated which categories of data were "included" among the data that was stolen by cyber criminals from the Defendants, but did not provide a list of all data categories that were involved:

> **What Information Was Involved?**
> Your affected information included, the date of birth, provider name, health insurance information, and treatment cost information.

54. To summarize, although the Defendants knew as early as June 1, 2023 that MOVEit software had a "vulnerability" and was compromised, and although they knew as early as July 6, 2023, that Delta Dental customers' information was involved in the Data Breach, they did not notify the Plaintiff and other victims of this Data Breach until January 12, 2024.

55. Upon information and belief, the Notice of Data Breach was drafted and publicized under the direction of PSC and Delta Dental.

56. Upon information and belief, PSC has sufficient control over the data which was stored and/or transported over PSC's file transfer software, MOVEit, to properly secure that data, but failed to do so. Upon information and belief, Plaintiff's and Class

Members' affected PII was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

57. It is likely the Data Breach was targeted at PSC due to its status as large information technology provider to businesses, including healthcare and financial service providers, such as Delta Dental, that collect, create, and maintain PII.

58. Defendants were untimely and unreasonably delayed in providing notice of the Breach to Plaintiff and Class Members.

59. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

60. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Delta Dental advised impacted individuals to "remain vigilant by reviewing your account statements and credit reports closely" and to follow the below steps to further protect themselves:

a. order your free credit report;

b. if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, contact the FTC and/or your

state's attorney general office about for information on how to prevent or avoid identity theft;

c. place a security freeze; and

d. place a fraud alert.

61. In particular, in the Notice of Data Breach letter, Delta Dental offered "24 months of free identity monitoring services through Kroll." This offer, made by Delta Dental, is woefully inadequate given that risks of identity theft do not expire within two years, and continue for a lifetime.

62. In sum, the Defendants largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

63. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[13]

64. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[14] leisure time is defined as time not occupied with work or chores and is "the time

---

[13] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed March 18, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, *https://www.bls.gov/news.release/pdf/wkyeng.pdf* (last accessed March 18, 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).

[14] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed March 18, 2024).

equivalent of 'disposable income.'"[15] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

65. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

66. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

67. Aside from the offer of 24 months of identity monitoring services, which is inadequate for reasons described above, Defendants have offered no measures to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for their respective lifetimes.

68. PSC and Delta Dental had and continue to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

---

[15] *Id.*

69. Plaintiff and the Class Members remain, even today, in the dark regarding the scope of the data breach, what particular data was stolen, beyond several categories listed in the letter as "included" in the Data Breach, the particular ransomware used, and what steps are being taken, if any, to secure their PII and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly the Defendants intend to enhance their information security systems and monitoring capabilities so as to prevent further breaches.

70. Plaintiff's and Class Members' PII and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

Defendants Failed to Comply with FTC Guidelines

71. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[16] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as PSC, should employ to protect against the unlawful exfiltration of PII.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[17] The guidelines explain that businesses should:

---

[16] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed March 18, 2024).

[17] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed March 18, 2024).

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

74. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[18]

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[18] *See Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 16, 2024).

76. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

77. Despite its alleged commitments to securing sensitive data, PSC does not follow industry standard practices in securing PII.

78. Experts studying cyber security routinely identify financial service providers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

79. Several best practices have been identified that at a minimum should be implemented by financial service providers like PSC, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

80. Other best cybersecurity practices that are standard in the financial service industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

81. PSC failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-

5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

82. Such frameworks are the existing and applicable industry standards in the financial service industry. PSC failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

83. Delta Dental failed to conduct minimal inquiry into PSC's data security practices before entrusting its clients' data to PSC, thus exposing them to the consequences of the Data Breach when it occurred.

The Experiences and Injuries of Plaintiff and Class Members

84. Plaintiff and Class Members are customers of Delta Dental, an entity that used PSC's MOVEit software.

85. As a prerequisite of using its services, Delta Dental requires its customers' customers—like Plaintiff and Class Members—to disclose their PII.

86. When Delta Dental finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Delta Dental's Breach Notice fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

87. Because of the Data Breach, Defendants inflicted injuries upon Plaintiff and Class Members. And yet, Defendants have done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

88. All Class Members were injured when PSC caused their PII to be exfiltrated by cybercriminals.

89. Plaintiff and Class Members entrusted their PII to Defendants. Thus, Plaintiff had the reasonable expectation and understanding that PSC would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. Plaintiff had reasonable expectation and understanding that Delta Dental would exercise reasonable care in selecting its data storage services provider. After all, Plaintiff would not have entrusted their PII to Defendants had they known that PSC would not take reasonable steps to safeguard their information.

90. Plaintiff and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that PSC obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

91. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

92. Plaintiff and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

93. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

94. Plaintiff and Class Members suffered injury from the misuse of their PII that can be directly traced to Defendants.

95. The ramifications of Delta Dental's selection of PSC as its data storage provider, and of PSC's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

96. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[19]

[19]Anne Saita, "Study Shows One in Four Who Receive Data Berach Letter Become Fraud Victims", Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited on March 18, 2024).

97. As a result of Defendants' failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of PSC and is subject to further breaches so long as PSC fails to undertake the appropriate measures to protect the PII in their possession.

98. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[20]

99. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

100. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

101. One such example of criminals using PII for profit is the development of "Fullz" packages.[21]

102. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope

---

[20] Brian Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on March 18, 2024).

[21] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, "Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm," KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/ (last visited on March 18, 2024).

and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

103. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

104. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

105. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendants did not rapidly report to Plaintiff and the Class that their PII had been stolen.

106. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

107. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

108. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

109. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[22]

110. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[23] According to the FTC, data security

---

[22] "Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable," FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on March 18, 2024).

[23] "Start With Security, A Guide for Business," FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 18, 2024).

requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[24]

111. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[25] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the "FTCA").

112. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. See *In the matter of Lookout Services, Inc.*, No. C-4326, Complaint ¶ 7 (June 15, 2011) ("[Respondent] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Respondent] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008)

[24] *Id.*

[25] "Taking Charge, What to Do If Your Identity is Stolen," U.S. DEPARTMENT OF JUSTICE, at 3 (January 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited on March 18, 2024).

("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Respondent] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . .").

113. These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendants thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

114. Charged with handling highly sensitive PII including, financial information, and insurance information, Defendants knew or should have known the importance of safeguarding the PII that was entrusted to it. Defendants also knew or should have known of the foreseeable consequences if their data security systems were breached. This includes the significant costs that would be imposed on Defendants' customers as a result of a breach. PSC nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring, and Delta Dental failed to inquire which, if any, security measures PSC employed to safeguard its clients' information before selecting PSC as its data storage services provider.

115. Delta Dental's selection of PSC as its data storage services provider, and PSC's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

116. Defendants' failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

117. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

118. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons residing in the United States who were clients of The Delta Dental of California or any of its affiliates, and whose PII was impacted by the Data Breach (the "Class").

119. The Class defined above is readily ascertainable from information in Defendants' possession. Thus, such identification of Class Members will be reliable and administratively feasible.

120. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendants or their

parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

121. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

122. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

123. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of tens of thousands of individuals who were clients of Delta Dental, or one of its member companies, and whose PII was compromised by PSC's Data Breach.

124. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. If PSC failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Delta Dental failed to adequately vet or otherwise inquire into PSC's data security practices before entrusting its clients' data to PSC;

d. If PSC's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

e. If PSC's data security systems prior to and during the Data Breach were consistent with industry standards;

f. If Defendants owed a duty to Class Members to safeguard their PII;

g. If Defendants breached their duty to Class Members to safeguard their PII;

h. If Defendants knew or should have known that PSC's data security systems and monitoring processes were deficient;

i. If Defendants should have discovered the Data Breach earlier;

j. If Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. If Defendants' delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Defendants' method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

m. If Defendants' conduct was negligent;

n. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

o. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

p. If Delta Dental breached its contracts with Plaintiff and Class Members;

q. If PSC breached implied contracts with Plaintiff and Class Members;

r. If Defendants was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

s. If Defendants failed to provide notice of the Data Breach in a timely manner; and

t. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

125. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to Defendants' uniformly illegal and impermissible conduct.

126. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

127. **Predominance**. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

128. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

129. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

130. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

131. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 124.

132. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

133. Plaintiff re-alleges and incorporate by reference paragraphs 1-132 of the Complaint as if fully set forth herein.

134. Defendants required Delta Dental's customers to submit Plaintiff's and Class Members' non-public PII to Defendants to receive Defendants' services.

135. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, PSC owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. PSC's duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

136. Delta Dental owed a duty to Plaintiff and Class Members to select a data storage services provider that employed reasonable data security measures to protect their

PII and other information. Delta Dental failed to conduct a reasonable, or any, inquiry when it selected PSC to store its clients' sensitive information.

137. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable to both Defendants. Given that PSC holds vast amounts of PII, it was inevitable that unauthorized individuals would at some point try to access PSC's databases of PII.

138. After all, PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, Defendants knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

139. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their, or their service providers', systems and networks, and the personnel responsible for them, adequately protected the PII.

140. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. Defendants were in a superior position to ensure that their, and their service providers', systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

141. Defendants failed to take appropriate measures to protect the PII of Plaintiff and the Class. Defendants are morally culpable, given the prominence of security breaches

in the financial services industry, including the insurance industry. Any purported safeguards that Defendants had in place were wholly inadequate.

142. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the financial service industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII. In addition, Delta Dental breached its duty to exercise its reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to conduct adequate due diligence on PSC's data security practices and procedures before engaging PSC as its data storage services provider.

143. The Defendants were negligent in failing to comply with industry and federal regulations in respect of safeguarding and protecting Plaintiff's and Class Members' PII.

144. But for Defendants' wrongful and negligent breach of their duties to Plaintiff and the Classes, Plaintiff's and Class Members' PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Classes and all resulting damages.

145. Defendants owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

146. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals who Defendants knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendants actively sought and obtained the PII of Plaintiff and Class Members.

147. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. In addition, Delta Dental breached its duties by failing to conduct an adequate inquiry into PSC's data security practices and procedures, before engaging PSC as its data storage services provider. But for Defendants' negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by Defendants include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to comply with—and thus violating—FTCA and its regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. For Delta Dental, failing to conduct an adequate inquiry into PSC's data security practices and procedures;

e. Failing to have in place mitigation policies and procedures;

f. Allowing unauthorized access to Class Members' PII;

g. Failing to detect in a timely manner that Class Members' PII had been compromised; and

h. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

148. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial service industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

149. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Defendants knew or should have known that their systems and technologies for processing and securing the PII of Plaintiff and the Classes had security vulnerabilities.

150. As a result of Defendants' negligence, the PII, PHI, and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII being disclosed to third parties without the consent of Plaintiff and the Class members.

151. Simply put, Defendants' negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of

their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

152. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

153. Plaintiff re-alleges and incorporates by reference paragraphs 1-132 of the Complaint as if fully set forth herein.

154. Under the Federal Trade Commission Act, Defendants had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[26]

155. Moreover, Plaintiff's and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that PSC inflicted upon Plaintiff and Class Members.

[26] 15 U.S.C. § 45.

156. Defendants' duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

157. Defendants' failure to comply with FTCA statutory duties and standards of conduct constitutes negligence *per se*. Defendants' failure to comply with the requisite standard of care caused the Breach, exposing Plaintiff's and Class Members' PII to cyber criminal and causing Plaintiff and Class Members pecuniary and non-pecuniary harm detailed herein.

158. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (1) strengthen their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for the remainders of their lives.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

159. Plaintiff re-alleges and incorporate by reference paragraphs 1-132 of the Complaint as if fully set forth herein.

160. This cause of action is plead in the alternative to the breach of implied contract theory.

161. Plaintiff and Class Members conferred a monetary benefit on Defendants, by paying money for Delta Dental services, a portion of which was passed on by Delta Dental to PSC, and was intended to have been used by Defendants for data security measures to

secure Plaintiff and Class Members' PII. Plaintiff and Class Members further conferred a benefit on Defendants in the form of their PII from which Defendants derived profits.

162. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of PSC's failure to provide adequate security.

163. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

164. Defendants acquired the monetary benefit, PII and PHI, through inequitable means in that Defendants failed to disclose their inadequate security practices, previously alleged, and failed to maintain adequate data security.

165. If Plaintiff and Class Members knew that Defendants had not secured their PII, they would not have agreed to give their money—or disclosed their data—to PSC or Delta Dental.

166. Plaintiff and Class Members have no adequate remedy at law.

167. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their

PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach.

168. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

169. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative, and the undersigned as Class Counsel;

B. A mandatory injunction directing Defendants to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete and purge the PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

v. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

vi. prohibiting Defendants from maintaining Plaintiff's and Class Members' PII on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is

compromised, hackers cannot gain access to other portions of Defendants' systems;

viii. requiring Defendants to conduct regular database scanning and securing checks;

ix. requiring Defendants to monitor ingress and egress of all network traffic;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xi. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with PSC's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor PSC's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendants to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the

steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. An injunction enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: March 25, 2024

Respectfully Submitted,

/s/ *Michael F. Ram*

Michael F. Ram
California Bar No: 104805
mram@forthepeople.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Ave, Ste 500,
San Francisco, CA, 94102-3275
T: (415) 846-3862

John A. Yanchunis*
JYanchunis@forthepeople.com
Ronald Podolny*
ronald.podolny@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

**Pro hac vice forthcoming*

Counsel for Plaintiff and the Class